Deutscher Bundestag **Drucksache 17/6765**

17. Wahlperiode 03. 08. 2011

Gesetzentwurf

des Bundesrates

Entwurf eines … Gesetzes zur Änderung des Telemediengesetzes (TMG)

A. Problem und Ziel

Das Thema Internet und vor allem die Telemediendienste, die den Nutzern eine Plattform bieten, um sich interaktiv mit anderen Nutzern auszutauschen, also Telemediendienste mit so genannten nutzergenerierten Inhalten, wie z. B. soziale Onlinenetzwerke oder auch Internetforen, haben für die Öffentlichkeit in den letzten Jahren immer mehr an Bedeutung gewonnen. Dennoch wird der Schutz privater Daten im Internet bislang häufig vernachlässigt, was vor allem daran liegt, dass der Datenschutz im Internet nicht ausreichend geregelt ist.

Ein großes Problem ist dabei zum einen immer noch die für Nutzer mangelnde Transparenz bei der Erhebung, Verarbeitung oder Nutzung persönlicher Daten durch die Internetanbieter. Ein Internetunternehmen ist nach § 13 Absatz 1 TMG zwar verpflichtet, die Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie darüber zu informieren, wenn die Verarbeitung der Daten in bestimmten Staaten außerhalb der EU stattfindet. Nicht geregelt ist dagegen, wo diese Informationen platziert werden müssen. Viele Internetdienstleister verstecken ihre Hinweise daher irgendwo in ihren Nutzungsbedingungen, so dass die Nutzer – wenn überhaupt – erst zufällig nach vielen Klicks darauf stoßen.

Zum anderen fehlt es oft auch an einer ausreichenden Aufklärung der Internetnutzer über die Risiken für Persönlichkeitsrechte bei der Preisgabe persönlicher Daten. Gerade bei Telemediendiensten mit nutzergenerierten Inhalten, wie z. B. den sozialen Netzwerken, machen sich die Nutzer häufig gar keine Gedanken über die Gefahren und bringen solchen Telemediendiensten blindes Vertrauen entgegen. Um alle Funktionen, die ein Telemediendienst mit nutzergenerierten Inhalten bietet, auch nutzen zu können, geben die Nutzer viel über sich und ihr Umfeld preis. Viele Nutzer, insbesondere Kinder und Jugendliche, unterschätzen dabei oft die erheblichen Gefahren für ihre Persönlichkeitsrechte und die Privatsphäre. Abgesehen von den Gefahren, die durch Kontakte im Internet entstehen können (z. B. Pädophile in Schüler-Netzwerken) ist auch vielen nicht bewusst, dass alle Daten und Fotos, die sie veröffentlichen, wie an einem Schwarzen Brett für die anderen Nutzer des Telemediendienstes, z. B. innerhalb eines sozialen Netzwerks, und unter Umständen über Internetsuchmaschinen für alle Internetnutzer sichtbar sind und weiterverwendet werden können. Die Probleme, die durch leichtfertig weitergegebene Informationen oder unbedachte Veröffentlichungen im Internet entstehen können, reichen von Identitätsdiebstahl bis hin zum Verlust des Arbeitsplatzes. Für diese Probleme müssen die Nutzer sensibilisiert werden.

Ein weiteres Problem ist schließlich die Frage, was mit den persönlichen Daten passiert, die einmal ins Internet gestellt wurden. „Das Internet vergisst nichts“ sollten sich Nutzer bewusst machen, denn solche Nutzerkonten sind dann für alle Zeiten im Internet, selbst wenn sie jahrelang nicht mehr aktiv genutzt worden sind. Eine Löschung des einmal angelegten Nutzerkontos und der darin enthaltenen persönlichen Daten bieten die Diensteanbieter oftmals nicht an, ebenso wenig eine Löschung bzw. Anonymisierung weiterer Daten, die gegebenenfalls mit dem Nutzerkonto in Verbindung stehen.

B. Lösung

Die Informationspflichten des Diensteanbieters gegenüber den Nutzern müssen verstärkt werden. Die Nutzer müssen jederzeit und auch ohne technisches Hintergrundwissen die Möglichkeit haben, datenschutzrechtliche Informationen zu erhalten. Wegen der besonderen Gefahren müssen Diensteanbieter von nutzergenerierten Inhalten, z. B. soziale Netzwerke, bei denen die Nutzer viele sehr persönliche Daten ins Internet einstellen können, zusätzliche Pflichten erfüllen. Standardmäßig soll der Diensteanbieter bei der Neuanmeldung eines Nutzers zunächst die höchste Sicherheitsstufe gemäß dem Stand der Technik voreinstellen, die von dem Nutzer dann gelockert werden kann, wenn er dies möchte. Eine besonders wichtige Voreinstellung, die Verhinderung der Auffindbarkeit und Auslesbarkeit mittels externer Suchmaschinen, wird vorgegeben. Auch durch die Aufklärung über die Risiken der Veröffentlichung persönlicher Daten soll der Nutzer sensibilisiert werden. Schließlich soll der Nutzer immer die Möglichkeit haben, selbst zu veranlassen, dass seine in dem Telemediendienst veröffentlichten Daten wieder gelöscht oder zumindest gesperrt bzw. anonymisiert werden.

C. Alternativen

Keine.

D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

Keine.

E. Sonstige Kosten

Keine.

BUNDESREPUBLIK DEUTSCHLAND
DIE BUNDESKANZLERIN

Berlin, 3. August 2011

An den
Präsidenten des
Deutschen Bundestages
Herrn Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich gemäß Artikel 76 Absatz 3 des Grundgesetzes den vom Bundesrat in seiner 884. Sitzung am 17. Juni 2011 beschlossenen

Entwurf eines ... Gesetzes zur Änderung des Telemediengesetzes (TMG)

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium für Wirtschaft und Technologie.

Die Auffassung der Bundesregierung zu dem Gesetzentwurf ist in der als Anlage 2 beigefügten Stellungnahme dargelegt.

Mit freundlichen Grüßen
Der Stellvertreter der Bundeskanzlerin

Philipp Rösler

Anlage 1

Entwurf eines … Gesetzes zur Änderung des Telemediengesetzes (TMG)

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Telemediengesetzes

Das Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist, wird wie folgt geändert:

1. § 2 Satz 1 wird wie folgt geändert:

   a) Nach Nummer 3 wird folgende Nummer 4 eingefügt:

   „4. ist Nutzerkonto das persönliche Datenkonto eines Nutzers bei einem Telemediendienst, bestehend aus Bestandsdaten nach § 14 Absatz 1 und gegebenenfalls zusätzlichen personenbezogenen Daten, die der Diensteanbieter bei dem Nutzer erhoben hat und verarbeitet, durch das der Nutzer die zugangsbeschränkten Funktionen dieses Telemediendienstes nutzen kann,“.

   b) Die bisherigen Nummern 4 bis 6 werden die Nummern 5 bis 7.

2. § 13 wird wie folgt geändert:

   a) Absatz 1 Satz 1 wird wie folgt gefasst:

   „Werden personenbezogene Daten des Nutzers erhoben, hat der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs in allgemein verständlicher Form, leicht erkennbar und unmittelbar erreichbar über

   1. Art, Umfang und Zwecke der Erhebung, Verarbeitung oder Nutzung seiner Daten,

   2. die Kategorien der Empfänger nur, soweit der Nutzer nach den Umständen des Einzelfalls nicht mit der Weitergabe an diese rechnen muss,

   3. die zuständige Aufsichtsbehörde für den Datenschutz und

   4. die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31), die durch die Verordnung (EG) Nr. 1882/2003 (ABl. L 284 vom 31.10.2003, S. 1) geändert worden ist,

   zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist.“

   b) Absatz 4 wird wie folgt geändert:

   aa) Satz 1 wird wie folgt gefasst:

   „Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass

   1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,

   2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des Satzes 3 gesperrt werden,

   3. der Nutzer die Löschung seines Nutzerkontos durch ein leicht erkennbares, unmittelbar erreichbares und ständig verfügbares Bedienelement jederzeit selbst veranlassen kann,

   4. im Falle der Nichtnutzung des Nutzerkontos das Nutzerkonto nach Ablauf des Jahres, das dem Jahr der letzten Nutzung folgt, gelöscht oder in den Fällen des Satzes 3 gesperrt werden,

   5. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,

   6. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,

   7. Daten nach § 15 Absatz 2 nur für Abrechnungszwecke zusammengeführt werden können und

   8. Nutzungsprofile nach § 15 Absatz 3 nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.“

   bb) Nach Satz 1 wird folgender Satz eingefügt:

   „Im Falle der Veranlassung einer Löschung nach Satz 1 Nummer 3 durch den Nutzer hat der Diensteanbieter das Nutzerkonto unverzüglich zu löschen, soweit nicht rechtliche Gründe einer Löschung des Nutzerkontos entgegenstehen, oder in den Fällen des Satzes 3 zu sperren.“

   cc) In dem neuen Satz 3 werden nach der Angabe „Satz 1 Nr. 2“ die Wörter „oder Nummer 4 oder Satz 2“ eingefügt.

   dd) Nach dem neuen Satz 3 werden folgende Sätze eingefügt:

   „Soweit eine Löschung nach Satz 1 Nummer 3 nicht möglich ist, hat der Diensteanbieter den Nutzer unverzüglich unter Angabe der Gründe

darüber zu unterrichten und mitzuteilen, zu welchem Zeitpunkt die Löschung des Nutzerkontos erfolgen wird. Im Falle der Löschung oder Sperrung eines Nutzerkontos nach Satz 1 Nummer 4 hat der Diensteanbieter den Nutzer spätestens vier Wochen vor der Löschung oder Sperrung über die beabsichtigte Maßnahme zu unterrichten.“

c) Folgender Absatz 8 wird angefügt:

„(8) Die Speicherung von Daten im Endgerät des Nutzers und der Zugriff auf Daten, die im Endgerät des Nutzers gespeichert sind, sind nur zulässig, wenn der Nutzer darüber entsprechend Absatz 1 unterrichtet worden ist und er hierin eingewilligt hat. Dies gilt nicht, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, um einen vom Nutzer ausdrücklich gewünschten elektronischen Informations- oder Kommunikationsdienst zur Verfügung stellen zu können.“

3. Nach § 13 wird folgender § 13a eingefügt:

„§ 13a
Zusätzliche Pflichten des Diensteanbieters von Telemediendiensten mit nutzergenerierten Inhalten

(1) Soweit der Diensteanbieter dem Nutzer die Möglichkeit bietet, den Telemediendienst durch eigene Inhalte mit personenbezogenen Daten zu erstellen und zu gestalten und diese Inhalte anderen Nutzern zugänglich zu machen (Telemediendienst mit nutzergenerierten Inhalten), hat der Diensteanbieter die Sicherheitseinstellungen auf der höchsten Sicherheitsstufe gemäß dem Stand der Technik voreinzustellen. Der Diensteanbieter hat den Nutzer bei der erstmaligen Erhebung von personenbezogenen Daten in allgemein verständlicher Form, leicht erkennbar, unmittelbar erreichbar und ständig verfügbar darüber zu unterrichten, welche Sicherheitseinstellungen zum Schutz der Privatsphäre des Nutzers voreingestellt sind. Der Diensteanbieter muss dem Nutzer die Einstellungsmöglichkeit bieten, dass das Nutzerkonto sowie sonstige vom Nutzer erstellte Inhalte mittels anderer, nicht in diesen Telemediendienst integrierter Telemediendienste, welche die Suche von Inhalten ermöglichen (externe Suchmaschinen), nicht gefunden oder ausgelesen werden können; der Diensteanbieter hat dies entsprechend Satz 1 voreinzustellen. Satz 3 gilt nicht, soweit der Zweck des Telemediendienstes bei objektiver Betrachtung die Auffindbarkeit oder Auslesbarkeit von Inhalten mittels externer Suchmaschinen umfasst. Einem Nutzer, der bei der Erhebung seiner personenbezogenen Daten ein Alter von unter 16 Jahren angegeben hat, darf eine Änderung der Voreinstellung nach Satz 3 erst ermöglicht werden, wenn er das Alter von 16 Jahren erreicht hat.

(2) Der Diensteanbieter des Telemediendienstes mit nutzergenerierten Inhalten hat den Nutzer

1. über mögliche Risiken für personenbezogene Daten und damit verbundene Beeinträchtigungen seiner Persönlichkeitsrechte und
2. darüber, dass durch das Zugänglichmachen von personenbezogenen Daten, insbesondere von Foto-, Video-, Ton- oder Textinhalten, weder die Persönlichkeitsrechte noch sonstige Rechte einer anderen natürlichen Person verletzt werden dürfen,

in für den Nutzer verständlicher Form, leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu unterrichten.

(3) Im Falle der Löschung eines Nutzerkontos nach § 13 Absatz 4 Satz 1 Nummer 4 oder Satz 2 ist der Diensteanbieter eines Telemediendienstes mit nutzergenerierten Inhalten verpflichtet, auch alle nutzergenerierten Inhalte eines Nutzers zu löschen. Soweit es sich um nutzergenerierte Inhalte handelt, die in Zusammenhang mit nutzergenerierten Inhalten anderer Nutzer stehen, tritt an die Stelle der Löschung die Anonymisierung. Eine Pflicht zur Löschung oder Anonymisierung besteht nicht, soweit eine Löschung oder Anonymisierung nach dem Verwendungszweck nicht möglich ist oder einen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

(4) § 13 bleibt unberührt.

(5) Das Bundesministerium für Wirtschaft und Technologie wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium des Innern zu bestimmen, welche Anforderungen gemäß dem Stand der Technik an die höchste Sicherheitsstufe der Sicherheitseinstellungen gemäß Absatz 1 Satz 1 zu stellen sind.“

4. § 16 Absatz 2 wird wie folgt geändert:

a) In Nummer 2 werden nach den Wörtern „§ 13 Absatz 1 Satz 1 oder 2“ die Wörter „oder Absatz 4 Satz 4 oder 5 oder § 13a Absatz 1 Satz 2 oder Absatz 2“ eingefügt.

b) Nummer 3 wird wie folgt gefasst:

„3. einer der in § 13 Absatz 4 Satz 1 Nummer 1 bis 6 oder 7 genannten Pflichten zur Sicherstellung zuwiderhandelt,“.

c) Nach Nummer 3 werden folgende Nummern 4 und 5 eingefügt:

„4. entgegen § 13 Absatz 4 Satz 2 nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig löscht oder sperrt oder entgegen § 13a Absatz 3 nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig löscht oder anonymisiert,

5. einer der in § 13a Absatz 1 Satz 1, 3 oder 5 genannten Pflichten zuwiderhandelt,“.

d) Die bisherigen Nummern 4 und 5 werden die Nummern 6 und 7.

Artikel 2
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeines

Das Thema Internet und vor allem die Telemediendienste, die den Nutzern eine Plattform bieten, um sich interaktiv mit anderen Nutzern auszutauschen, also Telemediendienste mit so genannten nutzergenerierten Inhalten, wie z. B. soziale Onlinenetzwerke oder auch Internetforen, haben für die Öffentlichkeit in den letzten Jahren immer mehr an Bedeutung gewonnen. Dennoch wird der Schutz privater Daten im Internet bislang häufig vernachlässigt, was vor allem daran liegt, dass der Datenschutz im Internet nicht ausreichend geregelt ist.

Ein großes Problem ist dabei zum einen immer noch die für Nutzer mangelnde Transparenz bei der Erhebung, Verarbeitung oder Nutzung persönlicher Daten durch die Internetanbieter. Ein Internetunternehmen ist nach § 13 Absatz 1 TMG zwar verpflichtet, die Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie darüber zu informieren, wenn die Verarbeitung der Daten in bestimmten Staaten außerhalb der EU stattfindet. Nicht geregelt ist dagegen, wo diese Informationen platziert werden müssen. Viele Internetdienstleister verstecken ihre Hinweise daher irgendwo in ihren Nutzungsbedingungen, so dass die Nutzer – wenn überhaupt – erst zufällig nach vielen Klicks darauf stoßen.

Zum anderen fehlt es oft auch an einer ausreichenden Aufklärung der Internetnutzer über die Risiken für Persönlichkeitsrechte bei der Preisgabe persönlicher Daten. Gerade bei Telemediendiensten mit nutzergenerierten Inhalten, wie z. B. den sozialen Netzwerken, machen sich die Nutzer häufig gar keine Gedanken über die Gefahren und bringen solchen Telemediendiensten blindes Vertrauen entgegen. Um alle Funktionen, die ein Telemediendienst mit nutzergenerierten Inhalten bietet, auch nutzen zu können, geben die Nutzer viel über sich und ihr Umfeld preis. Viele Nutzer, insbesondere Kinder und Jugendliche, unterschätzen dabei oft die erheblichen Gefahren für ihre Persönlichkeitsrechte und die Privatsphäre. Abgesehen von den Gefahren, die durch Kontakte im Internet entstehen können, z. B. Pädophile in Schüler-Netzwerken, ist auch vielen nicht bewusst, dass alle Daten und Fotos, die sie veröffentlichen, wie an einem schwarzen Brett für die anderen Nutzer des Telemediendienstes und unter Umständen über Internetsuchmaschinen für alle Internetnutzer sichtbar sind und weiterverwendet werden können. Die Probleme, die durch leichtfertig weitergegebene Informationen oder unbedachte Veröffentlichungen im Internet entstehen können, reichen von Identitätsdiebstahl bis hin zum Verlust des Arbeitsplatzes. Für diese Probleme müssen die Nutzer sensibilisiert werden.

Ein weiteres Problem ist schließlich die Frage, was mit den persönlichen Daten passiert, die einmal ins Internet gestellt wurden. „Das Internet vergisst nichts“ sollten sich Nutzer bewusst machen, denn solche Nutzerkonten sind dann für alle Zeiten im Internet, selbst wenn sie jahrelang nicht mehr aktiv genutzt worden sind. Eine Löschung des einmal angelegten Nutzerkontos und der darin enthaltenen persönlichen Daten bieten die Diensteanbieter oftmals nicht an, ebenso wenig eine Löschung bzw. Anonymisierung weiterer Daten, die gegebenenfalls mit dem Nutzerkonto in Verbindung stehen.

Der hier vorliegende Gesetzentwurf geht auf die Besonderheiten des Web 2.0 ein und stellt eine Reaktion auf den Paradigmenwechsel, der sich in den letzten Jahren im Internet vollzogen hat, dar. Das Internet ist nicht mehr geprägt durch Nutzer, die Informationen aus dem Internet nur konsumieren. Es hat sich durch das Web 2.0 zu einer Aktionsplattform für Nutzer entwickelt, die selbst agieren möchten und dadurch selbst zu einem Anbieter von Informationen werden. Diesem Schritt ist das TMG bisher noch nicht gefolgt, so dass dringender Ergänzungsbedarf bestand.

Es geht darum, Regelungen zu schaffen, die zwar die technischen Entwicklungen der letzten Jahre wiederspiegeln, jedoch trotzdem möglichst durch technikneutrale Begriffe geprägt sind, um keine Einzelfalllösung darzustellen. Die Nutzer werden durch die Möglichkeiten zwar faktisch selbst zu einem Anbieter von Informationen, dennoch dürfen die Pflichten des eigentlichen Diensteanbieters des Telemediendienstes nicht vernachlässigt werden. Der Diensteanbieter muss die Nutzer überhaupt erst in die Lage versetzen, ihre Verantwortung sich selbst und anderen gegenüber auch ausüben zu können, indem er sie informiert und ihnen gestalterische Möglichkeiten bietet.

B. Zu den einzelnen Vorschriften

Zu Artikel 1 (Änderung des Telemediengesetzes)

Zu Nummer 1 (§ 2 TMG)

Zu Buchstabe a

Unter Nummer 4 werden die Definitionen um den Begriff des Nutzerkontos ergänzt.

In den letzten Jahren haben so genannte zugangsbeschränkte Telemediendienste im Internet enorm zugenommen. Zugangsbeschränkte Telemediendienste sind Telemediendienste, die nur von Nutzern mit einem Nutzerkonto – einem so genannten account – genutzt werden können bzw. die Nutzern, die über kein Nutzerkonto verfügen, nur sehr eingeschränkte Nutzungsmöglichkeiten bieten, z. B. Lese- statt Schreibrechte in Foren. Das Einrichten eines Nutzerkontos kann erforderlich sein, um im Internet Einkäufe tätigen zu können, z. B. Bahn, Amazon, ebay etc., aber auch in sozialen Netzwerken wie Facebook, „wer-kennt-wen“, den VZ-Gruppen oder allgemein in Internetforen und auf Diskussionsplattformen ist das Anlegen eines Nutzerkontos zwingend erforderlich, um den Dienst nutzen zu können. Der Zugang zu einem dem Nutzer zugeordneten Nutzerkonto ist nur möglich, wenn der Nutzer sich durch die Eingabe bestimmter Daten, in der Regel Benutzername oder E-Mail-Adresse und Passwort, als zugangsberechtigt ausgewiesen hat.

Um ein Nutzerkonto zu erhalten, muss der Nutzer sich bei dem Telemediendienst registrieren. Dafür ist meist vorgesehen, dass der Nutzer dem Diensteanbieter gegenüber per-

sonenbezogene Daten wie Name und E-Mail-Adresse, oft auch Wohnort und weitere Informationen, angibt.

Für den Begriff der Bestandsdaten ist die Definition des § 14 Absatz 1 heranzuziehen, nach der es sich bei „Bestandsdaten“ um personenbezogene Daten eines Nutzers handelt, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind. Die §§ 14, 13 Absatz 6 bleiben unberührt, d. h. inwieweit der Nutzer gezwungen werden darf, personenbezogene Daten anzugeben, richtet sich nach den genannten Vorschriften.

Alle personenbezogenen Daten, die der Diensteanbieter bei dem Nutzer darüber hinaus erhebt und verarbeitet, können also nur auf freiwilliger Basis erhoben und verarbeitet werden, z. B. Hobbies, Beruf, Schule, persönliche Interessen, private Telefonnummern, der Hinweis auf eine eigene Homepage usw. Soweit es sich bei den Daten des Nutzerkontos um personenbezogene Daten handeln sollte, die ausnahmsweise der Inhaltsebene nach dem Bundesdatenschutzgesetz (BDSG) zuzuordnen sind, sind auch hier die geltenden Vorschriften im Hinblick auf die Zulässigkeit der Erhebung und Verarbeitung der Daten zu berücksichtigen.

Zu Buchstabe b

Es handelt sich um redaktionelle Folgeänderungen.

Zu Nummer 2 (§ 13 TMG)

Zu Buchstabe a

§ 13 Absatz 1 Satz 1 sieht für die Diensteanbieter weitergehende Unterrichtungspflichten vor. Inhaltlich orientiert sich die neue Regelung am Aufbau und an den Formulierungen des § 4 Absatz 3 BDSG, behält jedoch – soweit möglich – inhaltlich die alte Fassung des § 13 Absatz 1 Satz 1 TMG bei. Aus Sicht der Aufsichtspraxis war Satz 1 der alten Fassung insbesondere wegen der verschachtelten Formulierung nicht aus sich heraus hinreichend verständlich.

In Anlehnung an die allgemeinen Informationspflichten in § 5 Absatz 1 TMG müssen die Datenschutzhinweise in allgemein verständlicher Form, leicht erkennbar und unmittelbar erreichbar sein. Der Nutzer muss die Datenschutzhinweise unzweifelhaft als solche erkennen können. Sie dürfen nicht im Impressum, in den Allgemeinen Geschäfts- bzw. Nutzungsbedingungen oder auch sonstigen allgemeinen Erläuterungen versteckt sein, sondern müssen gesondert aufgeführt werden. Sie sind unmittelbar erreichbar, wenn der Nutzer sie spätestens nach dem zweiten Klick gefunden hat. Das Erreichen einer Internetseite über zwei Links erfordert regelmäßig noch kein langes Suchen (vgl. BGH, Urteil vom 20. Juli 2006 – Az.: I ZR 228/03 – zur Anbieterkennzeichnung im Internet).

Vergleichbar der Regelung in § 4 Absatz 3 Nummer 3 BDSG müssen nunmehr auch in den Datenschutzhinweisen nach dem TMG die Kategorien von Empfängern genannt werden (§ 13 Absatz 1 Satz 1 Nummer 2). Grund dafür ist, dass der Nutzer einen Überblick bekommen soll, ob und gegebenenfalls an welche Dienstleister seine Daten weitergegeben werden. Dass nicht jeder einzelne Dienstleister genannt werden muss, vereinfacht dem Diensteanbieter die praktische Anwendung. Der Diensteanbieter ist nicht gezwungen, bei jedem Wechsel eines Dienstleisters seinen Internetauftritt zu ändern und anzupassen. Für den Nutzer reicht es aus, die Kategorien der Empfänger zu erfahren, da er meist schon anhand dieser Informationen einschätzen kann, ob sie mit einer Weitergabe seiner personenbezogenen Daten an die genannten Kategorien von Empfängern einverstanden ist. Entgegen der in § 4 Absatz 3 Nummer 3 BDSG verwendeten Formulierung, die im zweiten Halbsatz auf eine „Übermittlung“ abstellt, wird in der vorliegenden Fassung der Begriff der „Weitergabe“ verwendet. Aus Sicht der Aufsichtspraxis ist der Begriff „Übermittlung“ in § 4 Absatz 3 Nummer 3 BDSG eine sprachliche Unschärfe, da eine Übermittlung entsprechend der Definition in § 3 Absatz 4 Nummer 3 BDSG nur an Dritte erfolgen kann, die Regelung jedoch weiter geht und alle Empfänger betrifft.

Die neu eingeführte Nummer 3 des § 13 Absatz 1 Satz 1 dient der Benutzerfreundlichkeit. Indem der Diensteanbieter künftig im Rahmen seines Internet-Auftritts die für ihn zuständige Stelle für die Datenschutzaufsicht benennen muss, ist der Nutzer bei Beschwerden oder einen Diensteanbieter betreffende Anfragen nicht mehr selbst zur umfangreichen Recherche gezwungen. Da jedes Land über eine eigene Datenschutzaufsicht verfügt, war für den Nutzer oft unklar, welche Behörde zuständig ist. Ein weiterer positiver Effekt ist die schnellere Bearbeitung, denn Eingaben bei der unzuständigen Stelle, die nach den Erfahrungen aus der Aufsichtspraxis bisher häufig vorgekommen sind, können dadurch weitgehend vermieden werden.

Die Formulierung des § 13 Absatz 1 Satz 1 Nummer 4 ist unverändert geblieben.

Zu Buchstabe b

Zu Doppelbuchstabe aa

Um zu verhindern, dass einmal eingegebene persönliche Daten der Nutzer für alle Zeiten im Internet verbleiben, gefunden und gegebenenfalls missbraucht werden können, werden dem Diensteanbieter in § 13 Absatz 4 Satz 1 Nummer 3 und 4 neue Pflichten im Hinblick auf die Löschung von personenbezogenen Daten auferlegt.

Neben die bereits bestehende Verpflichtung des Diensteanbieters nach § 13 Absatz 4 Satz 1 Nummer 2, dafür zu sorgen, dass die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung (so genannte Nutzungsdaten) gelöscht werden, tritt nun auch die Verpflichtung, eine Löschfunktion für den Nutzer bereit zu halten, die es dem Nutzer ermöglicht, die Löschung seines Nutzerkontos jederzeit selbst zu veranlassen (§ 13 Absatz 4 Satz 1 Nummer 3). Das Bedienelement („Löschknopf“) muss leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein, so dass der Nutzer die Löschung jederzeit selbst veranlassen kann. Im Hinblick auf die Definitionen zur leichten Erkennbarkeit, unmittelbaren Erreichbarkeit und ständigen Verfügbarkeit wird auf die Ausführungen zu Nummer 3 Buchstabe a (§ 13 Absatz 1 Satz 1 TMG) verwiesen. Eine selbständige Löschung des Nutzerkontos und der darin enthaltenen personenbezogenen Daten durch den Nutzer, wie sie in den letzten Jahren immer wieder gefordert wird, dürfte derzeit technisch nicht umsetzbar sein, so dass das Betätigen des Löschknopfes dem Nutzer lediglich die Möglichkeit bietet, dem Diensteanbieter auf einfache Art

und Weise mitteilen zu können, dass das Nutzerkonto gelöscht werden soll. Die Löschung selbst muss dann durch den Diensteanbieter erfolgen.

Der Löschknopf bietet zwei Vorteile: Erstens muss der Löschknopf nunmehr von allen Telemediendiensten bereit gestellt werden, während bisher nur wenige Diensteanbieter überhaupt eine Löschmöglichkeit des Nutzerkontos angeboten haben. Zweitens ist die Veranlassung einer Löschung durch einen Löschknopf für den Nutzer wesentlich einfacher, als wenn er gezwungen ist, den Diensteanbieter per Brief oder E-Mail zu benachrichtigen, damit das Nutzerkonto gelöscht wird.

Ferner wird eine Löschroutine für Nutzerkonten, wenn diese über einen längeren Zeitraum nicht mehr aktiv genutzt wurden, vorgegeben (§ 13 Absatz 4 Satz 1 Nummer 4). Als ausreichend wird ein Zeitraum von ein bis zwei Jahren angesehen, in dem das Konto nicht genutzt wurde, bemessen ab dem Datum des letzten „Einloggens“, also Anmeldens, bei dem Telemediendienst. Wenn der Nutzer sich mit seinem Nutzerkonto z. B. letztmalig im Juni 2010 bei dem Telemediendienst eingeloggt hat und danach keine weitere Aktivitäten auf dem Nutzerkonto erfolgen, ist der Diensteanbieter verpflichtet, das Nutzerkonto nach Ablauf des Jahres 2011, also am 1. Januar 2012, zu löschen.

Eine Regelung, die flexibel den jeweiligen Zeitpunkt der letzten Nutzung berücksichtigt, wäre für den Diensteanbieter mit einem unverhältnismäßigen Aufwand verbunden. Eine einmal im Jahr ablaufende Löschroutine wird als ausreichend angesehen. Auch der Nutzer wird durch diese Löschroutine nicht unverhältnismäßig benachteiligt. Zwar ist der Nutzer dadurch ggf. gezwungen, seine Daten ein zweites Mal bei einem Diensteanbieter einzugeben, wenn die letzte Nutzung zu weit zurücklag und seine Daten bereits gelöscht wurden. Eine solche Löschung kann der Nutzer jedoch einfach vermeiden, indem er regelmäßig, zumindest einmal im Jahr, auf dem jeweiligen Nutzerkonto aktiv wird. Es reicht dafür aus, sich einmal kurz ein- und gleich wieder auszuloggen. Im Hinblick auf den umfassenden Schutz, der durch die Löschroutine erreicht werden kann, ist ein derartiger Aufwand dem Nutzer durchaus zumutbar, wenn er ein Interesse an einem bestimmten Nutzerkonto hat und dessen Löschung verhindern möchte. Wenn die Daten wegen gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen nicht gelöscht werden können, muss das Nutzerkonto zumindest gesperrt werden. Die Regelung ist wortgleich zu § 13 Absatz 4 Satz 1 Nummer 2.

Die Nummern 5 bis 8 – alt – erhalten eine neue Nummerierung, bleiben jedoch inhaltlich unverändert.

Zu Doppelbuchstabe bb

Die neue Regelung wurde eingefügt, um einem Missbrauch der Löschfunktion entgegenzuwirken. Es wird klargestellt, dass eine Löschung des Nutzerkontos nur dann möglich ist, wenn dieser Löschung keine rechtlichen Gründe entgegenstehen. Mit dieser Regelung soll verhindert werden, dass sich ein Nutzer z. B. noch bestehender Forderungen oder offener Rechnungen des Diensteanbieters dadurch zu entziehen versucht, dass er sein Nutzerkonto löscht und der Diensteanbieter seine Ansprüche gegenüber dem Nutzer nicht mehr geltend machen könnte.

Der Begriff „unverzüglich“ bedeutet, dass eine Handlung ohne schuldhaftes Zögern erfolgt (siehe § 121 Absatz 1 Satz 1 des Bürgerlichen Gesetzbuchs). Entscheidend ist dabei nicht die objektive, sondern die subjektive Zumutbarkeit des alsbaldigen Handelns. Es ist zwar nicht erforderlich, dass eine Handlung sofort vorgenommen wird, da dem Handelnden eine angemessene Überlegungsfrist eingeräumt wird. Als Obergrenze wird von den Gerichten in der Regel ein Zeitraum von zwei Wochen angesehen.

Zu Doppelbuchstabe cc

Da – ebenso wie nach § 13 Absatz 4 Nummer 2 – auch bei § 13 Absatz 4 Nummer 4 statt einer Löschung eine Sperrung in Betracht kommen kann, wenn Aufbewahrungsfristen einer Löschung der Daten entgegenstehen, handelt es sich bei der Einfügung unter § 13 Absatz 4 Satz 3 lediglich um eine redaktionelle Folgeänderung.

Zu Doppelbuchstabe dd

Die nach Satz 3 neu eingefügten Sätze 4 und 5 legen dem Diensteanbieter weitere Unterrichtungspflichten im Hinblick auf Satz 1 Nummer 3 und 4 auf.

Wenn ein Nutzer die Löschung seines Nutzerkontos nach Satz 1 Nummer 3 veranlasst hat, obwohl einer Löschung rechtliche Gründe entgegenstehen, muss der Diensteanbieter dem Nutzer dies aus Transparenzgründen mitteilen (Satz 4). Wichtig ist, dass auch die Unterrichtung „unverzüglich“, also in der Regel innerhalb eines Zeitrahmens von zwei Wochen, erfolgen muss (s. o. zu Doppelbuchstabe dd). Der Diensteanbieter muss dem Nutzer die Gründe nennen, die einer sofortigen Löschung des Nutzerkontos entgegenstehen. Dies bietet dem Nutzer zum einen die Möglichkeit, Abhilfe zu schaffen, um dann eine Löschung des Nutzerkontos durchsetzen zu können, z. B. indem der Nutzer eine noch offene Rechnung begleicht. Zum anderen kann dadurch auch die Argumentation des Diensteanbieters einer Überprüfung unterzogen werden, denn ohne Angabe von Gründen könnte der Diensteanbieter ansonsten missbräuchlich die Löschung eines Nutzerkontos verweigern.

Auch im Falle der Löschung eines Nutzerkontos nach Absatz 4 Satz 1 Nummer 4 besteht für den Diensteanbieter eine Unterrichtungspflicht (Satz 5). Bevor der Diensteanbieter seiner Verpflichtung nachkommen und das Nutzerkonto eines Nutzers unwiderruflich löschen darf, hat er den betroffenen Nutzer darüber zu unterrichten, dass eine Löschung beabsichtigt ist. Die Mitteilung muss mindestens vier Wochen vor der Löschung erfolgen, da dem Nutzer noch ein angemessener Zeitrahmen zur Verfügung stehen soll, um ggf. entsprechende Gegenmaßnahmen einzuleiten. Falls er die Löschung verhindern möchte, muss sich der Nutzer lediglich einmal kurz ein- und wieder ausloggen, um das Nutzerkonto erneut zu aktivieren.

Zu Buchstabe c

Absatz 8 setzt Artikel 5 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation; ABl. L 201 vom 31.7.2002, S. 37, in der konsolidier-

ten Fassung vom 19. Dezember 2009) um. Mit der Regelung werden Nutzer davor geschützt, dass ohne ihre Einwilligung Daten auf ihrem Endgerät gespeichert werden oder auf dort gespeicherte Daten zugegriffen wird.

Zu Nummer 3 (§ 13a TMG)

§ 13a legt bestimmten Diensteanbietern weitergehende Pflichten auf.

Unter einem Telemediendienst mit nutzerdefinierten Inhalten sind alle Telemediendienste zu verstehen, die den Nutzern die Möglichkeit bieten, selbst Daten oder Inhalte zu veröffentlichen. Viele Diensteanbieter bieten den Nutzern dabei die Möglichkeit, eine Art Steckbrief der eigenen Person (im Internet häufig „Profil" genannt) zu erstellen, der von anderen Nutzern eingesehen werden kann, z. B. in den sozialen Netzwerken. Zu einem solchen „Profil" gehören neben dem Namen viele persönliche Angaben wie z. B. Hobbies, Schule, Beruf, persönliche Interessen, private Telefonnummern, der Hinweis auf eine eigene Homepage etc., um den Nutzern so die Möglichkeit zu bieten, miteinander in Kontakt zu treten, z. B. wegen gemeinsamer Interessen oder auch nur, um alte Freunde wiederzufinden. Oftmals wird dem Nutzer auch die Möglichkeit geboten, neben einem „Profil" noch Fotoalben, Videos, Musik oder ähnliches hochzuladen und ins Internet zur Veröffentlichung einzustellen. Die nutzergenerierten Inhalte können teilweise Bestandteil des Nutzerkontos sein, gehen aber meist auch deutlich darüber hinaus.

Absatz 1 betrifft die Sicherheitseinstellungen zum Schutz der Privatsphäre des Nutzers. Zwar gibt es inzwischen – zumindest in den meisten sozialen Netzwerken – Einstellungsmöglichkeiten, die es dem Nutzer ermöglichen, zu entscheiden, welche Information welchen anderen Nutzern zugänglich sein sollen. Diese Sicherheitseinstellungen waren bisher meist auf die niedrigste Sicherheitsstufe eingestellt, so dass alle personenbezogenen Daten einschließlich der Fotos für andere Nutzer öffentlich zugänglich waren. Es bestand jederzeit das Risiko eines Missbrauchs der Daten. Um ein seinen Interessen entsprechendes Schutzniveau zu erreichen, war der Nutzer gezwungen, die Einstellungen zum Schutz seiner Privatsphäre entsprechend zu ändern.

Durch die neue Regelung in Satz 1 hat der Diensteanbieter nicht mehr die Möglichkeit, frei zu entscheiden, welches Schutzniveau er im Rahmen der Voreinstellung wählt. Er ist verpflichtet, seine Sicherheitseinstellungen so einzustellen, dass für den Nutzer das höchste Schutzniveau nach dem Stand der Technik erreicht wird. Dies ist erforderlich, da es sich immer wieder gezeigt hat, dass die Nutzer sich mit den Sicherheitseinstellungen – gerade zu Beginn der Nutzung – noch gar nicht auseinandersetzen können oder wollen und oftmals in der Vergangenheit auch die entsprechenden Einstellungsmöglichkeiten nicht oder nur schlecht auffindbar waren. Durch die Festlegung, dass zunächst die höchste Sicherheitsstufe voreingestellt sein muss, wird dem Nutzer die Möglichkeit gegeben, sich zunächst mit den Funktionen und Möglichkeiten des Telemediendienstes vertraut zu machen und dann zu entscheiden, welche der vorgegebenen Sicherheitseinstellungen er eventuell lockern möchte.

Damit der Nutzer die Sicherheitseinstellungen eines Telemediendienstes angemessen beurteilen und einschätzen kann, muss der Diensteanbieter den Nutzer über die Voreinstellungen unterrichten (Satz 2). Sofern der Nutzer entsprechend informiert ist, kann er sich dann entweder für einen Diensteanbieter mit hohen Sicherheitsvorkehrungen oder für einen Diensteanbieter mit einem geringen Schutzniveau entscheiden. Wichtig ist, dass der Nutzer diese Entscheidung bewusst und unter Berücksichtigung aller vorhandenen Möglichkeiten treffen kann.

Hinsichtlich des Zeitpunktes der Unterrichtung wird auf die „erste Erhebung von personenbezogenen Daten" abgestellt. Da der Diensteanbieter bereits im Rahmen der Registrierung erstmalig personenbezogene Daten des Nutzers erhält, muss der Nutzer auch bereits zu diesem Zeitpunkt darüber informiert werden, welche Sicherheitseinstellungen der Diensteanbieter dem Nutzer bietet. Ein früherer Zeitpunkt wäre für den Nutzer irreführend, denn solange er einen Telemediendienst nur „passiv" nutzt, also z. B. auf dessen Homepage „surft", benötigt er noch keine Informationen zu den Sicherheitseinstellungen der zugangsbeschränkten Funktionen. Diese Sicherheitseinstellungen werden für den Nutzer erst dann wichtig und interessant, wenn der Diensteanbieter erstmalig Daten bei dem Nutzer erhebt und verarbeitet. Zu diesem Zeitpunkt muss der Nutzer wissen, welche Sicherheitseinstellungen voreingestellt sind, damit er anhand dieser Informationen entscheiden kann, ob er das Angebot des Diensteanbieters nutzen und welche Daten er veröffentlichen möchte.

Von der Regel, dass dem Diensteanbieter mit nutzergenerierten Inhalten grundsätzlich keine Vorgaben hinsichtlich der Mindeststandards gemacht werden, sieht Satz 3 eine Ausnahme vor. Er regelt die Suchfunktion im Internet im Zusammenhang mit den Telemediendiensten mit nutzergenerierten Inhalten und schreibt dem Diensteanbieter vor, dass weder das Nutzerkonto noch sonstige von dem Nutzer erstellte Inhalte im Rahmen einer Suche durch eine externe Suchmaschine, wie z. B. Google oder Bing, standardmäßig gefunden oder ausgelesen werden dürfen. Das bedeutet, es dürfen in den externen Suchmaschinen weder die persönlichen Daten des Nutzers angezeigt, noch darf überhaupt ein Hinweis auf eine entsprechende Mitgliedschaft bei einem derartigen Telemediendienst gegeben werden.

Durch die Formulierung „durch ein anderes, nicht in diesen Telemediendienst integrierten Telemediendienst" werden Suchfunktionen innerhalb des Telemediendienstes nicht erfasst, die dem internen Auffinden von Informationen dienen, z. B. eine Suchmaschine innerhalb eines sozialen Netzwerks. Telemediendienste mit nutzergenerierten Inhalten sind darauf angelegt, dass die Nutzer aus einer Fülle von Informationen die für sie interessanten herausfiltern können. Dies ist größtenteils nur durch entsprechende Suchfunktionen möglich, z. B. wenn ein Nutzer einen früheren Freund in einem sozialen Netzwerk wiederfinden möchte oder auch zu einem bestimmten Thema entsprechende Ansprechpartner gesucht werden. Der letzte Halbsatz in Satz 3, nach dem der Diensteanbieter diesen Mindeststandard auf die höchste Sicherheitsstufe voreinzustellen hat, dient lediglich der Klarstellung, da sich die entsprechende Verpflichtung dazu bereits aus Satz 1 ergibt.

Der Mindeststandard nach Satz 3 gilt jedoch nicht für alle Diensteanbieter mit nutzergenerierten Inhalten. Nach Satz 4 gilt Satz 3 nicht, soweit der Zweck des Telemediendienstes bei objektiver Betrachtung die Auffindbarkeit oder Ausles-

barkeit von Inhalten mittels externer Suchmaschinen umfasst. Dies betrifft z. B. Diensteanbieter von Diskussionsforen und Blogs wie Twitter. Derartige Angebote dienen dem Zweck, andere Nutzer über bestimmte Themen zu informieren und sind daher bei objektiver Betrachtung grundsätzlich darauf ausgerichtet, dass sie mittels externer Suchmaschinen aufgefunden und ausgelesen werden können. Es wäre unverhältnismäßig, alle Diensteanbieter solcher Angebote zu zwingen, eine technische Möglichkeit zur Nichtauffindbarkeit durch Suchmaschinen zu schaffen, wenn der gesamte Dienst auf eine Veröffentlichung und damit auch auf eine Auffindbarkeit und Auslesbarkeit im Internet ausgerichtet ist. Auch den Nutzern, die Beiträge in einem Blog schreiben, geht es darum, dass diese Beiträge von einer möglichst großen Nutzer wahrgenommen werden. Dies ist in einem solchen Umfang nur durch das Auffinden durch Suchmaschinen möglich. In der Regel wird der Verfasser eines Beitrages in einem Forum auch kein Interesse daran haben, die Suchmaschinenfunktion erst freischalten zu müssen.

Hinsichtlich von Foren muss jedoch differenziert werden. Während allgemein zugängliche Foren dem öffentlichen Austausch von Meinungen und Gedanken dienen, unterliegen z. B. Foren innerhalb eines sozialen Netzwerks anderen Regeln. In einem solchen Netzwerk, das in sich den Anschein der Geschlossenheit hat, sind viele Nutzer bereit, Informationen und Meinungen preiszugeben, die sie in einem allgemein zugänglichen Forum vielleicht nicht geäußert hätten. Die Verfasser der Beiträge in einem solchen Forum bedürfen daher eines besonderen Schutzes, so dass sie nicht unter die Ausnahme des Satzes 4 fallen. Foren innerhalb eines Telemediendienstes dürfen daher ebenso wie die persönlichen Profile der Nutzer nicht von einer externen Suchmaschine aufgefunden und ausgelesen werden können, um einem anderen Nutzer nicht durch die Anzeige eines Beitrags in einem Forum auf die Mitgliedschaft in einem sozialen Netzwerk und die dort vorhandenen Informationen über eine Person hinzuweisen.

Nicht von der Ausnahmeregelung des Satzes 4 erfasst werden soziale Netzwerke, die berufliche Kontakte vermitteln können (z. B. „Xing“). Zwar dienen solche Netzwerke dem Zweck, berufliche Kontakte zu vermitteln; eine solche Kontaktaufnahme ist jedoch nicht zwingend nur durch eine externe Suchmaschine möglich. Die Suche kann vielmehr auch auf dem „klassischen Weg“ des Suchens in dem entsprechenden sozialen Netzwerk erfolgen, so dass eine grundsätzliche Nichtauffindbarkeit mittels Suchmaschinen der Funktionsweise des sozialen Netzwerkes an sich nicht entgegensteht, zumal die Nutzer jederzeit die Möglichkeit haben, die vorgegebenen Sicherheitseinstellungen zu ändern und auf den entsprechenden Schutz zu verzichten.

Für Nutzer unter 16 Jahren geht der Schutz nach Satz 3 dagegen sogar noch weiter. Satz 5 sieht vor, dass Nutzer, die noch nicht 16 Jahre alt sind, keine entsprechende Einwilligung zur Auslesbarkeit und Auffindbarkeit in Suchmaschinen geben dürfen. Da eine Überprüfung der Angaben eines Nutzers derzeit noch nicht problemlos möglich ist, ist dieser Schutz auf die Nutzer beschränkt, die im Rahmen der Anmeldung ein Alter von unter 16 Jahren angegeben haben. Weitergehende Verpflichtungen zur Überprüfung des angegebenen Alters werden dem Diensteanbieter nicht auferlegt.

Nach Absatz 2 muss der Nutzer über die Risiken der Veröffentlichung unterrichtet werden. Es geht dabei zum einen um die Risiken, die dem Nutzer selbst drohen, wenn er unbedacht persönliche Daten oder auch Fotos von sich preisgibt. Peinliche Partyfotos oder Fotos von Personen mit Alkohol können z. B. leicht dazu führen, dass ein potentieller Arbeitgeber einen Bewerber ablehnt. Auch bei Veröffentlichungen von Beiträgen in Foren drohen Nachteile, z. B. kann der Antrag eines Nutzers auf Abschluss eines Versicherungsvertrags daran scheitern, dass der Nutzer unter seinem Klarnamen in einem Forum über bestehende Vorerkrankungen diskutiert, die er in dem Antrag nicht angegeben hat. All dies sind Risiken, über die sich die Nutzer im Allgemeinen keinerlei Gedanken machen und über die sie aufgeklärt werden müssen. Zum anderen geht es dabei aber auch um die Risiken, die dem Nutzer drohen, wenn er unüberlegt Fotos von anderen Personen im Internet veröffentlicht, ohne vorher deren Einwilligung eingeholt zu haben. Den meisten Nutzern ist heutzutage gar nicht bewusst, dass sie eine Einwilligung benötigen, wenn sie Fotos von einer anderen Person veröffentlichen wollen. Sollte die Person mit der Veröffentlichung nicht einverstanden sein, kann es schlimmstenfalls sogar zu Rechtsstreitigkeiten kommen und ggf. können Schadensersatzansprüche entstehen. Auch auf solche Risiken muss der Nutzer aufmerksam gemacht werden.

Wegen der besonderen Risiken, die mit einer unbedachten Veröffentlichung im Internet verbunden sein können, müssen die Warnhinweise nicht nur in allgemein verständlicher, sondern in einer für den Nutzer verständlichen Form angeboten werden. Das bedeutet, der Diensteanbieter ist verpflichtet, die Informationen so zu präsentieren, dass sie von dem „typischen Nutzer“ seines Dienstes verstanden werden kann. Der Diensteanbieter eines Telemediendienstes, der sich hauptsächlich an Jugendliche richtet, kann damit verpflichtet sein, andere Formulierungen zur Erklärung zu verwenden als ein Diensteanbieter, dessen Dienst sich z. B. vorzugsweise an Senioren richtet. Sonst besteht das Risiko, dass vor allem Jugendliche sich von den Warnhinweisen nicht angesprochen fühlen und diese ignorieren. Auch hier hat der Diensteanbieter dafür zu sorgen, dass die Warnhinweise so platziert werden, dass der Nutzer sie jederzeit ohne Aufwand auffinden und einsehen kann.

Absatz 3 betrifft die Löschung bzw. Anonymisierung von nutzergenerierten Inhalten im Falle einer Löschung des Nutzerkontos.

Telemediendienste mit nutzergenerierten Inhalten, wie z. B. soziale Netzwerke, bieten ihren Nutzern die Möglichkeit, auf einer entsprechenden Plattform eigene Inhalte zu veröffentlichen bzw. hochzuladen und damit einer unbekannten Anzahl von Nutzern zur Ansicht zur Verfügung zu stellen. Dies geschieht häufig vor allem durch eine persönliche Darstellung in Form eigener Fotos, der persönlichen Lieblingsmusik, eigener Videos oder auch durch Veröffentlichung der eigenen Meinung in Gästebüchern, Diskussionsrunden oder Foren.

Für solche personenbezogenen Daten, die nicht zwingend dem Nutzerkonto zugerechnet werden können, insbesondere wenn es sich um Diskussions- oder Gästebucheinträge handelt, greift weder die Löschmöglichkeit durch den Nutzer nach § 13 Absatz 4 Satz 1 Nummer 3 noch die automatische Löschroutine nach § 13 Absatz 4 Satz 1 Nummer 4. Es besteht somit die Gefahr, dass solche Daten auch nach der

Löschung eines Nutzerkontos im Internet erhalten bleiben und noch Jahre später der Eintrag eines Nutzers im Internet gefunden werden kann. Absatz 3 dient daher der Klarstellung, dass auch solche Daten zwingend gelöscht werden müssen. Der Nutzer muss die Gewissheit haben, dass all die Daten, die er durch den Diensteanbieter innerhalb des Telemediendienstes anderern Nutzern zugänglich gemacht habt, wieder gelöscht werden, egal um welche Information es sich handelt und in welchem Bereich innerhalb des Telemediendienstes sie veröffentlicht wurden.

Von diesem Grundsatz sieht Satz 2 eine Ausnahme vor, die Veröffentlichungen der Nutzer in Zusammenhang mit den Veröffentlichungen anderer Nutzer betreffen. In einem solchen Fall ist statt der Löschung eine Anonymisierung der personenbezogenen Daten vorzunehmen. Während es in der Regel keine Probleme bereiten dürfte, im Rahmen der Löschung eines Nutzerkontos auch Fotoalben, die der Nutzer auf seiner persönlichen Seite im Internet veröffentlicht hat, zu löschen, ist dann mit Schwierigkeiten zu rechnen, wenn es um Meinungsäußerungen in einer Diskussionsrunde geht. Solche Äußerungen sind nur dann verständlich, wenn auch der gesamte Kontext zu einem Thema veröffentlicht wird. Wenn Nutzer A z. B. zu einem Thema seine Meinung kundtut und Nutzer B in seinem Beitrag dieser Aussage zustimmt. Der Beitrag von Nutzer B wäre nicht mehr verständlich, wenn die Meinung von Nutzer A gelöscht werden würde und könnte sich evtl. sogar unbeabsichtigt auf eine entgegengesetzte Meinung in einem anderen Beitrag beziehen. Die Alternative, alle Beiträge zu einem Thema zu löschen, wenn einer der Teilnehmer die Löschung seines Beitrages wünscht, ist schon aus Gründen der Meinungsfreiheit der anderen Teilnehmer keine Option. Da es dem Betroffenen in erster Linie darum geht, den Äußerungen im Internet nicht mehr zugeordnet werden zu können, ist eine Anonymisierung ausreichend, um die Privatsphäre des Nutzers zu schützen. Die insoweit vorzunehmende Anonymisierung nach Maßgabe des § 3 Absatz 6 BDSG erfordert, dass personenbezogene Daten wie der Name des Verfassers eines Beitrages in einem Forum derart verändert werden, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Die Möglichkeit der Anonymisierung scheidet dann aus, wenn dies nach dem Verwendungszweck unmöglich ist oder im Verhältnis zu dem angestrebten Schutzzweck einen unverhältnismäßigen Aufwand bedeutet (Satz 3). Welche Maßnahme unverhältnismäßig ist, ist eine Frage des Einzelfalls und hat sich – wie in § 9 BDSG – an den Bezugsgrößen „Schutzzweck und Aufwand“ zu orientieren. Unverhältnismäßigkeit könnte z. B. gegeben sein, wenn der Diensteanbieter alle Beiträge eines Nutzers einzeln durchsuchen und jeden Beitrag gesondert anonymisieren müsste. Finanzielle Zusatzkosten, die durch die Einrichtung einer entsprechenden Funktion bei dem Telemediendienst entstehen, sind nicht zwingend unverhältnismäßig.

Absatz 4 stellt klar, dass die Verpflichtungen des Diensteanbieters nach § 13 unberührt bleiben.

Absatz 5 schafft die Möglichkeit, die Anforderungen an die höchste Sicherheitsstufe durch Bestimmung des Standes der Technik zu konkretisieren.

Zu Nummer 4 (§ 16 Absatz 2 TMG)

Zu Buchstabe a

Die Vorschrift des § 16 Absatz 2 Nummer 2 wird ergänzt, indem auch ein Verstoß gegen die neu eingefügten Unterrichtungspflichten nach § 13 Absatz 4 Satz 4 und Satz 5, nach § 13a Absatz 1 Satz 2 sowie nach § 13a Absatz 2 als Ordnungswidrigkeiten geahndet werden können.

Zu Buchstabe b

Ein Verstoß gegen die neu eingeführten Pflichten in Bezug auf die Löschmöglichkeit durch den Nutzer und das Unterlassen einer regelmäßigen Löschroutine bei einem Nutzerkonto, das längere Zeit nicht mehr genutzt wurde, sind bußgeldbewehrt. Dem Nutzer die Möglichkeit einzuräumen, die Löschung seines Nutzerkontos selbst veranlassen zu können, ohne erst den Diensteanbieter per E-Mail oder per Brief um Löschung bitten zu müssen, ist im Rahmen der heutigen technischen Möglichkeiten ohne größeren Aufwand umsetzbar. Auch die regelmäßige Löschung nicht genutzter Nutzerkonten wird einmal pro Jahr ohne Weiteres möglich sein.

Zu Buchstabe c

Die neu eingefügte Bußgeldvorschrift der Nummer 4 betrifft die Löschungspflichten des Diensteanbieters nach § 13 Absatz 4 Satz 2 und § 13a Absatz 3. Nach § 13 Absatz 4 Satz 2 ist der Diensteanbieter verpflichtet, das Nutzerkonto eines Nutzers unverzüglich zu löschen oder zumindest zu sperren, sobald der Nutzer dies durch das Ausüben der Löschfunktion veranlasst hat. Nach § 13a Absatz 3 hat der Diensteanbieter noch weitergehende Pflichten dahingehend, dass er im Falle der Löschung eines Nutzerkontos auch alle nutzergenerierten Inhalte löschen oder zumindest anonymisieren muss.

Die neu eingefügte Bußgeldvorschrift der Nummer 5 betrifft die Pflichten des Diensteanbieters in Bezug auf die Sicherheitseinstellungen. Bußgeldbewehrt ist ein Verstoß gegen § 13a Absatz 1 Satz 1, wonach der Diensteanbieter verpflichtet ist, die Voreinstellung auf der von ihm angebotenen höchsten Sicherheitsstufe vorzunehmen. Ebenso bußgeldbewehrt ist es, wenn der Diensteanbieter dem Nutzer nicht die Möglichkeit einer Sicherheitseinstellung bietet, die das Auffinden und Auslesen des Nutzerkontos mittels externer Suchmaschinen verhindert (§ 13a Absatz 1 Satz 3) oder wenn der Diensteanbieter einem Nutzer, der ein Alter von unter 16 Jahren angegeben hat, die Möglichkeit einräumt, die Voreinstellungen hinsichtlich der Nichtauffindbarkeit und Nichtauslesbarkeit mittels externer Suchmaschinen zu ändern (§ 13a Absatz 1 Satz 5). Es handelt sich dabei um entscheidende Pflichten, die dem Schutz der personenbezogenen Daten der Nutzer dienen. Ein Verstoß dagegen muss daher auch mittels Bußgeld sanktionierbar sein.

Zu Buchstabe d

Es handelt sich um redaktionelle Folgeänderungen.

Zu Artikel 2 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes.

Anlage 2

Stellungnahme der Bundesregierung

A. Allgemeines

Der in seiner Sitzung am 17. Juni 2011 vom Bundesrat beschlossene Gesetzentwurf zur Änderung des Telemediengesetzes (Bundesratsdrucksache 156/11 (Beschluss)) zielt auf einen verbesserten Datenschutz bei Telemedienangeboten mit nutzergenerierten Inhalten, insbesondere bei sozialen Netzwerken ab. Dazu schlägt er umfangreiche Änderungen im Telemediengesetz (TMG) vor. Kernanliegen ist die Einfügung eines neuen § 13a TMG, der eine Reihe zusätzlicher Pflichten für Anbieter von Telemedien mit nutzergenerierten Inhalten enthält.

Der Gesetzentwurf greift wichtige Themen auf, die den Datenschutz bei Internetangeboten mit nutzergenerierten Inhalten, insbesondere sozialen Netzwerken betreffen. Die Bundesregierung teilt die Ansicht, dass insofern und insbesondere mit Blick auf einen effektiven Kinder und Jugendmedienschutz ein besonders hohes Datenschutzniveau angestrebt werden sollte. Der Vorstoß des Bundesrates wirft jedoch zum jetzigen Zeitpunkt Fragen auf, die zunächst der Klärung bedürfen. Hierzu sollte aus Sicht der Bundesregierung zunächst die geltende Rechtslage einer intensiven Prüfung unterzogen werden, um zum Einen den tatsächlich bestehenden gesetzgeberischen Handlungsbedarf genauer zu ermitteln. Dabei sind alle datenschutzrechtlichen relevanten Normen zu berücksichtigen, also sowohl das Bundesdatenschutzgesetz (BDSG) als auch Regelungen des bereichsspezifischen Datenschutzes im Telekommunikations- und Telemedienrecht. Die Bundesregierung ist zum Anderen der Auffassung, dass den besonderen Herausforderungen an den Schutz der personenbezogenen Daten im Internetzeitalter auch auf europäischer Ebene begegnet werden sollte. Insbesondere können europaweit harmonisierte Bedingungen leichter international durchgesetzt werden als nationale Regelungen.

Die Bundesregierung erwartet in Kürze Vorschläge der Europäischen Kommission zur Neuregelung des europäischen Datenschutzrechts. Sie wird sich neben nationalen Überlegungen zur Verbesserung des Datenschutzes im Internet in den dann anstehenden Beratungen im Rat und gegenüber dem Europäischen Parlament für rechtliche Standards einsetzen, die insbesondere das Vertrauen der Internetnutzer in den wirksamen Schutz ihrer Persönlichkeitsrechte und den Datenschutz in sozialen Netzwerken stärken.

B. Zu den einzelnen Vorschlägen

1. Der Bundesrat möchte zusätzlich zu den bisherigen Begriffsbestimmungen den des „Nutzerkontos“ einführen (Artikel 1 Nummer 1 des Gesetzentwurfs). Der Begriff bezieht sich auf Telemediendienste, die ihre Informationen nur Nutzern zugänglich machen, die sich bei diesem Telemediendienst unter Angabe bestimmter persönlicher Informationen zuvor registrieren. Es trifft zu, dass viele Telemediendienste die Inanspruchnahme von einer solchen vorherigen Registrierung abhängig machen. Die „Nutzerkonten“ sind allerdings unterschiedlich ausgestaltet und enthalten verschiedene Daten, die auch rechtlich differenziert zu betrachten sind. Dabei kann neben dem bereichsspezifischen Datenschutzrecht im TMG auch allgemeines Datenschutzrecht anwendbar sein.

   Nach Auffassung der Bundesregierung besteht keine Regelungslücke, da die in einem „Nutzerkonto“ gespeicherten Informationen entweder im Rahmen des Anwendungsbereichs des TMG von dem in § 14 TMG geregelten Begriff der Bestandsdaten erfasst werden oder als Inhaltsdaten den Regelungen des BDSG unterfallen. Ob personenbezogene Daten gemäß § 14 TMG für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind oder ob es sich um Daten handelt, die darüber hinausgehend ggf. dem BDSG unterfallen, ist in jedem Einzelfall zu prüfen.

   Bei Überlegungen zur Schaffung neuer gesetzlicher Regelungen ist jeweils sorgfältig abzuwägen, ob es sich dabei um Inhalts- oder Bestandsdaten handelt und ob diese systematisch dem Regelungsbereich des BDSG oder des TMG zu unterwerfen sind. Die entsprechende Differenzierung wird im Gesetzentwurf des Bundesrates nicht ausreichend vorgenommen.

2. Der Bundesrat schlägt vor, § 13 Absatz 1 Satz 1 TMG neu zu fassen (Artikel 1 Nummer 2 Buchstabe a des Gesetzentwurfs). Die Vorschrift enthält in ihrer geltenden Fassung Unterrichtungspflichten, die Anbieter von Telemediendiensten erfüllen müssen, wenn sie personenbezogene Daten verwenden wollen. Der Bundesrat zielt in seinem Vorschlag auf zusätzliche Unterrichtungspflichten, und zwar hinsichtlich der Kategorien der Empfänger, soweit der Nutzer nach den Umständen des Einzelfalls nicht mit der Weitergabe an diese rechnen muss, sowie hinsichtlich der zuständigen Aufsichtsbehörde für den Datenschutz. Weiterhin soll die Unterrichtung zusätzlich leicht erkennbar und unmittelbar erreichbar sein.

   a) § 13 Absatz 1 Satz 1 TMG erhielt seine jetzige Fassung durch Artikel 3 Nummer 4 des Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 14. Dezember 2001 (BGBl. I S. 3721), seinerzeit noch bezogen auf eine Änderung des Teledienstedatenschutzgesetzes, das mit dem TMG aufgehoben wurde. Diese Fassung wurde in enger Bund-Länder-Abstimmung unter Einbeziehung der Datenschutzaufsichtsbehörden entwickelt. Der Bundesregierung sind seither keine Defizite hinsichtlich der bestehenden Regelung, die einen zusätzlichen gesetzlichen Handlungsbedarf begründen, bekannt geworden.

   b) Im Hinblick auf die leichte Erkennbarkeit und unmittelbare Erreichbarkeit der Datenschutzhinweise zielt

der Vorschlag des Bundesrates darauf ab, dass die Unterrichtung nicht im Impressum, in den Allgemeinen Geschäfts- bzw. Nutzungsbedingungen oder auch sonstigen allgemeinen Erläuterungen versteckt sein darf, sondern gesondert aufgeführt werden muss. Unter Bezugnahme auf die Rechtsprechung des Bundesgerichtshofs zur Anbieterkennzeichnung sieht der Bundesrat die unmittelbare Erreichbarkeit dann gegeben, wenn die Datenschutzinformationen spätestens nach dem zweiten Klick gefunden werden können.

Die Bundesregierung stimmt dem Bundesrat darin zu, dass klare rechtliche Vorgaben zu den Datenschutzhinweisen sowohl hinsichtlich der Ausübung des Rechts auf informationelle Selbstbestimmung seitens der Nutzer wie auch hinsichtlich der Rechtssicherheit der Anbieter unerlässlich sind. Es bestehen keine inhaltlichen Einwände gegen das Anliegen des Bundesrates, auch die leichte Erkennbarkeit und die unmittelbare Erreichbarkeit der Datenschutzhinweise gesetzlich zu regeln. Allerdings sollte insoweit gerade mit Blick auf den grenzüberschreitenden Charakter der Dienste der Informationsgesellschaft zunächst auf EU-weit harmonisierte Regeln hingewirkt werden. Auch hinsichtlich der vom Bundesrat als Beispiel zitierten Anbieterkennzeichnung bestehen EU-Vorgaben aus der E-Commerce-Richtlinie (Richtlinie 2000/31/EG). Die Bundesregierung wird sich bei den anstehenden Beratungen für ein neues EU-Datenschutzrecht für entsprechende Bestimmungen auf europäischer Ebene einsetzen.

3. Der Vorschlag zur Unterrichtung über Kategorien von Empfängern zielt darauf ab, dass der Nutzer einen Überblick bekommen soll, ob und gegebenenfalls an welche Dienstleister seine Daten weitergegeben werden. Dabei soll dem Diensteanbieter die Aufgabe dadurch vereinfacht werden, dass nicht jeder einzelne Empfänger benannt wird, sondern nur Kategorien. Das geltende Recht kennt, insbesondere in § 13 Absatz 1 Satz 1 TMG sowie in den §§ 33, 34 BDSG, bereits umfangreiche Unterrichtungs-, Benachrichtigungs- und Auskunftspflichten über die Verarbeitung von personenbezogenen Daten, insbesondere auch über ihre Weitergabe an Dritte. In den entsprechenden Regelungen ist der im nunmehr vom Bundesrat beschlossenen Gesetzentwurf verankerte Gedanke, die Informationen nach Kategorien von Empfängern zu staffeln, zum Teil bereits enthalten. Der Vorschlag des Bundesrates kann dahingehend verstanden werden, dass Diensteanbieter Nutzer zukünftig nicht nur über die Weiterleitung ihrer Daten an externe Dritte, sondern auch über die interne Weiterleitung von Daten im Verantwortungsbereich des Diensteanbieters informiert werden soll. Aus Sicht der Bundesregierung besteht jedoch aus Gründen des Datenschutzes keine Notwendigkeit dafür, dass der Diensteanbieter den Nutzer über seine Betriebsstruktur zu informieren hat. Sinnvoll könnte hingegen eine Information über die Empfänger im Rahmen der Auftragsdatenverwaltung sein, weil diese zwar keine Dritten im Sinne der oben genannten Vorschriften sind, es für die Nutzer aber eine wesentliche Information ist, ob die Daten von einem Anbieter selbst verwaltet werden oder ob dieser sich hierzu Dritter im Rahmen der Auftragsdatenverwaltung bedient. In diesem Sinn wird sich die Bundesregierung auf europäischer Ebene um Regelungen bemühen, die entsprechend dem Vorschlag des Bundesrates eine Pflicht der Diensteanbieter gegenüber den Nutzern zur Unterrichtung über Kategorien von Empfängern vorsehen, soweit diese nicht Teil des Unternehmens sind.

4. Im Hinblick auf den Vorschlag des Bundesrates, dass über die zuständige Aufsichtsbehörde unterrichtet werden soll, weist die Bundesregierung darauf hin, dass die Datenschutzaufsicht bei Telemedien den Ländern obliegt. Nach Artikel 28 der europäischen Datenschutz-Richtlinie 95/46/EG können die Mitgliedstaaten eine oder mehrere Kontrollstellen mit der Datenschutzaufsicht betrauen. Artikel 28 Absatz 4 der Datenschutzrichtlinie bestimmt jedoch zugleich, dass sich jede Person oder ein sie vertretender Verband zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden kann. In Deutschland müssten also alle 16 Datenschutzaufsichtsbehörden genannt werden, da aus Sicht der betroffenen Person jede dieser Behörden zuständig ist. Die Bundesregierung befürwortet durchaus, dass der Nutzer geeignete Informationen zu den bestehenden Rechtsschutzmöglichkeiten und Institutionen erhält. Sie hält es für sinnvoll, dass sich die zuständigen Aufsichtsbehörden über den Inhalt einer solchen Information verständigen und unter Geringhaltung des damit verbundenen Bürokratieaufwandes auf eine freiwillige Bereitstellung seitens der Diensteanbieter hinwirken.

5. Der Bundesrat schlägt vor, dass der Diensteanbieter durch technische und organisatorische Vorkehrungen sicherstellt, dass ein Nutzerkonto auf jederzeitige Veranlassung des Nutzers oder im Falle der Nichtnutzung nach einem Jahr automatisch gelöscht oder gesperrt wird (Artikel 1 Nummer 2 Buchstabe b des Gesetzentwurfs).

   Die Bundesregierung teilt die Auffassung, dass die Nutzer das Recht haben sollten, selbst eingestellte Inhalte auch wieder zu löschen. Gleiches gilt grundsätzlich für Nutzerkonten, unabhängig davon, ob und in welchem Umfang man diese unter den Begriff der Bestandsdaten gemäß § 14 TMG, unter den vom Bundesrat vorgeschlagenen neuen Begriff des „Nutzerkontos“ oder unter den Begriff der Inhaltsdaten im Sinne des BDSG fasst. Nach geltendem Recht besteht bereits eine Reihe von Löschungsansprüchen Die Bundesregierung wird sich auf europäischer Ebene für eine Harmonisierung im Sinne eines vollständigen Löschungsrechts, wie es im Gesetzentwurf des Bundesrates vorgesehen ist, einsetzen. Dies hätte zudem den Vorteil, dass ein solches Recht dann auch für ausländische Anbieter gelten würde.

6. Der Bundesrat schlägt einen neuen § 13 Absatz 8 TMG vor, der auf eine explizite Umsetzung von Artikel 5 Absatz 3 der europäischen E-Privacy-Richtlinie (Richtlinie 2002/58/EG) abzielt (vgl. Artikel 1 Nummer 2 Buchstabe c des Gesetzentwurfs). Die Vorschrift stellt Anforderungen u. a. an die Verwendung von so genannten Cookies.

   Die Bundesregierung prüft derzeit, wie durch eine Regelung im TMG Artikel 5 Absatz 3 der E-Privacy-Richtli-

nie umgesetzt werden kann. Sie wird dem Deutschen Bundestag – im Zuge der bereits im parlamentarischen Verfahren befindlichen Novellierung des Telekommunikationsgesetzes (TKG) – hierzu eigene Vorschläge unterbreiten.

7. Der vom Bundesrat vorgeschlagene neue § 13a TMG bildet das Hauptanliegen des Gesetzentwurfs. Darin werden zusätzliche Pflichten für Anbieter von Telemedien mit nutzergenerierten Inhalten geregelt (vgl. Artikel 1 Nummer 3 des Gesetzentwurfs). Insbesondere sollen die betroffenen Diensteanbieter

   - Sicherheitseinstellungen auf der höchsten Sicherheitsstufe gemäß dem Stand der Technik vorher einstellen,
   - unterrichten, welche Sicherheitseinstellungen zum Schutz der Privatsphäre des Nutzers voreingestellt sind,
   - die Einstellungsmöglichkeit anbieten, dass das Nutzerkonto sowie sonstige vom Nutzer erstellte Inhalte nicht von externen Suchmaschinen gefunden oder ausgelesen werden können und entsprechende Voreinstellung für Nutzer unter 16 Jahren,
   - die Nutzer über Risiken für Datenschutz und Persönlichkeitsrechte der Nutzer und Dritter unterrichten und
   - alle nutzergenerierten Inhalte des Nutzers im Fall der Löschung des Nutzerkontos löschen bzw. anonymisieren.

   a) Die Bundesregierung ist wie der Bundesrat der Auffassung, dass insbesondere das Phänomen der sozialen Netzwerke den Datenschutz im Internet vor besondere Herausforderungen stellt und insofern Regelungen erforderlich macht. Der Bundesregierung ist die Problematik von Voreinstellungen mit niedrigen Sicherheits- und Datenschutzstandards in sozialen Netzwerken bekannt. Hieraus ergeben sich zweifellos Risiken, insbesondere für Kinder und Jugendliche.

   b) Die Bundesregierung weist darauf hin, dass beispielsweise der erfolgreichste Anbieter von sozialen Netzwerken in Deutschland – Facebook – ein Unternehmen mit Sitz in Irland ist. Für Unternehmen, die ihren Sitz in einem anderen EU-Mitgliedstaat haben, gilt in Umsetzung von Artikel 4 der Richtlinie 95/46/EG in der Regel das Datenschutzrecht des Landes, in dem das Unternehmen seinen Sitz hat (vgl. § 1 Absatz 5 Satz 1 BDSG). Auch wenn man die Anwendbarkeit des deutschen Datenschutzrechts auf das Unternehmen Facebook bejahen sollte, stellt sich ein erhebliches Durchsetzungsproblem, da die Behörden eines Mitgliedstaates die Dienstleistungsfreiheit eines Dienstes der Informationsgesellschaft in einem anderen Mitgliedstaat nach dem Herkunftslandprinzip der E-Commerce-Richtlinie nur unter engen Voraussetzungen einschränken dürfen (vgl. § 3 Absatz 5 TMG).

   Die Situation auf dem Markt für soziale Netzwerke spricht daher dafür, dass auch hier – zumindest begleitend zu nationalen Bestrebungen – zunächst Lösungen auf europäischer Ebene gesucht werden sollten. Die Bundesregierung wird sich daher bei den anstehenden Beratungen zu einer europäischen Datenschutzrechtsreform dafür einsetzen und insbesondere eine Regelung zu datenschutzfreundlichen Voreinstellungen auf höchster Stufe anstreben.

   c) Es ist auch zu berücksichtigen, dass ein Verhaltenskodex der Betreiber von sozialen Netzwerken (vom 11. März 2009) existiert, dem sich die großen deutschen Anbieter „lokalisten.de“, die „VZ-Netzwerke“ und „wer-kennt-wen.de“ angeschlossen haben.

   Dieser Kodex bezieht sich bereits auf Forderungen wie etwa die Nichtauffindbarkeit des Profils durch externe Suchmaschinen bei Jugendlichen unter 16 Jahren, die standardmäßige Voreinstellung der strengsten Privatsphäreeinstellung bei Nutzern unter 14 Jahren, eine einfach zu findende Abmeldefunktion und Aufklärungshinweise etwa im Hinblick auf die Einhaltung von Urheber- und Persönlichkeitsrechten. Daher tritt das vom Bundesrat adressierte Problem, jedenfalls im Hinblick auf jugendliche Nutzer, bei den o. g. Betreibern von sozialen Netzwerken nicht auf. Facebook wird hingegen aus den oben genannten Gründen nicht erreicht.

   Die Bundesregierung befürwortet solche Selbstregulierungsinitiativen. Die Wirtschaft sollte dazu ermutigt werden, ihre Initiative zu zusätzlichen verbraucherfreundlichen Regelungen (z. B. Grundeinstellung auf dem strengsten Sicherheits- und Datenschutzniveau) fortzusetzen.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333